

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-338798

(43)Date of publication of application : 10.12.1999

(51)Int. Cl.

G06F 13/00

// H04L 9/08

(21)Application number : 10-146372

(71)Applicant : NTT COMMUNICATION WARE
KK

(22)Date of filing : 27.05.1998

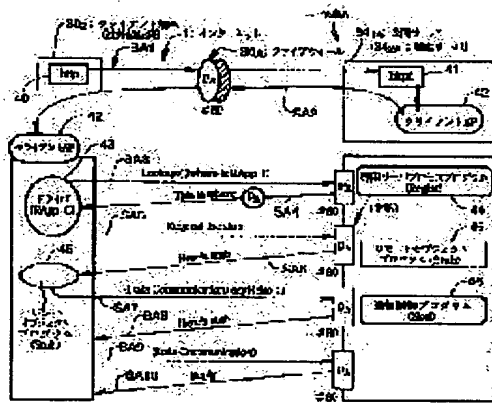
(72)Inventor : NAGAOKA TORU
SAKATA MASAFUMI
KOBAYASHI KAZUE

(54) NETWORK SYSTEM AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer readable recording medium recording a network system program without requiring an original security dedicated port for the security setting of a fire wall.

SOLUTION: This system is provided with a certified client terminal 302 and a secret server 342A connected through a fire wall 35A0 to an internet 1, and an http 40 from the client terminal 302 is inputted through a port PA of a port number #80 to the secret server 342A. After a specified client application program (AP) 42 is downloaded to the client terminal 302, the secret server 342A reports the information of the port PA to use a protocol sequence to the client terminal 302. Afterwards, data communication is performed between the client terminal 302 and the secret server 342A through the internet 1 and the port PA by a dedicated protocol.



LEGAL STATUS

[Date of request for examination] 23.03.2001

[Date of sending the examiner's
decision of rejection] 13.07.2004[Kind of final disposal of application
other than the examiner's decision of

rejection or application converted
registration]

[Date of final disposal for
application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-338798

(43) 公開日 平成11年(1999)12月10日

(51) Int.Cl.^{*}
G 0 6 F 13/00識別記号
3 5 1F I
G 0 6 F 13/00

3 5 1 H

3 5 1 Z

// H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 C

審査請求 未請求 請求項の数 5 O L (全 13 頁)

(21) 出願番号 特願平10-146372

(22) 出願日 平成10年(1998)5月27日

(71) 出願人 397065480

エヌ・ティ・ティ・コミュニケーションウ
ェア株式会社

東京都港区港南一丁目9番1号

(72) 発明者 長岡 亨

東京都港区港南一丁目9番1号 エヌ・テ
ィ・ティ・コミュニケーションウェア株式
会社内

(72) 発明者 坂田 雅史

東京都港区港南一丁目9番1号 エヌ・テ
ィ・ティ・コミュニケーションウェア株式
会社内

(74) 代理人 弁理士 志賀 正武 (外2名)

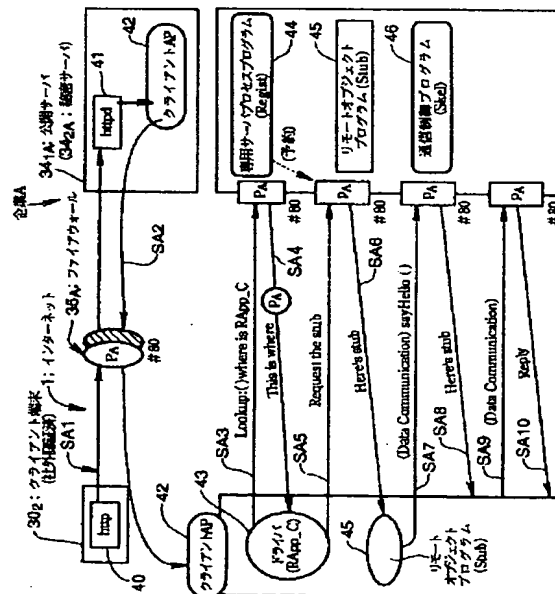
最終頁に続く

(54) 【発明の名称】 ネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムプログラムを記録したコンピュータ読み取り可能な記録媒体を得ること。

【解決手段】 本発明は、認証済のクライアント端末302と、ファイアウォール35Aを介してインターネット1に接続された秘密サーバ342Aとを備え、クライアント端末302からのhttp 40は、ポート番号#80のポートPAを通過して秘密サーバ342Aに入力される。秘密サーバ342Aは特定のクライアントAP（アプリケーションプログラム）42をクライアント端末302にダウンロードした後、プロトコルシーケンスを使用するポートpAの情報をクライアント端末302に通知する。以後専用のプロトコルによりインターネット1およびポートpAを介してクライアント端末302と秘密サーバ342Aとの間でデータ通信が行われる。



【特許請求の範囲】

【請求項1】 ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、

前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うことを特徴とするネットワークシステム。

【請求項2】 ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第1のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第1のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第2のポートとして設定し、

前記プロキシサーバは、前記クライアント端末から見たポートを前記第1のポートから前記第2のポートに変換する一方、前記サーバから見たポートを前記第2のポートから前記第1のポートに変換し、

前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うことを特徴とするネットワークシステム。

【請求項3】 前記クライアント端末に設けられ、前記データ通信におけるデータの暗号化および復号化を行う第1の暗号化通信制御部と、

前記サーバに設けられ、前記データ通信におけるデータの暗号化および復号化を行う第2の暗号化通信制御部と、

を具備することを特徴とする請求項1または2に記載のネットワークシステム。

【請求項4】 ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

10 前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、

前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項5】 ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

30 前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第1のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第1のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第2のポートとして設定し、

前記プロキシサーバは、前記クライアント端末から見たポートを前記第1のポートから前記第2のポートに変換する一方、前記サーバから見たポートを前記第2のポートから前記第1のポートに変換し、

40 前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

50 【発明の属する技術分野】本発明は、クライアント端末

からネットワークを介してサーバへのアクセスに用いられるネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】従来より、企業内におけるLAN（ローカルエリアネットワーク）環境においては、基幹業務に必要な多種多様なプロトコルが使用されているため、LAN等のシステムをインターネットを介して接続することは、後述するファイアウォールにおけるプロトコルの通過の可否等の問題から困難であった。しかしながら、近時、分散コンピューティング技術の浸透、Javaの普及により、インターネットを介して企業間LAN等のシステムを接続することによりネットワークシステムを構築することが可能になっている。ここで、このようなネットワークシステムを構築する場合には、ファイアウォールを設置することにより、セキュリティを確保している。

【0003】ここで、ファイアウォールとは、情報システムの本体とインターネットとの結合部分に設けられ、防火壁の役割を持つシステムであって、権限のない者の不正侵入の防止、コンピュータ・ウィルスの防止を行うものをいう。また、上述したファイアウォールを有するネットワークシステムにおいては、この環境下で使用できるプロトコル種別に対して、セキュリティポリシーに沿った制限を課すことにより、任意のプロトコルを通過させないことにより、セキュリティを確保している。

【0004】図5は、上述した従来のネットワークシステムの概略構成を示す図である。この図において、1は、複数のネットワークが互いに接続されてなるインターネットであり、図5に示す例では、インターネット1は、企業AのLANと企業BのLANとを接続している。企業Aにおいて、2は、各種のデータベースを記憶部に保持するデータベースサーバであり、ファイアウォール3を介してインターネット1に接続されている。

【0005】このデータベースサーバ2に対しては、認証された端末のみがファイアウォール3を介してアクセスすることができる。一方、未認証の端末は、ファイアウォール3を通過してデータベースサーバ2にアクセスできないようになっている。4は、インターネット1に接続された公開WWW（World Wide Web）サーバであり、認証、未認証を問わずいずれの端末であってもアクセス可能とされている。

【0006】一方、企業Bにおいて、5は、各種データベースを記憶部に保持するデータベースサーバであり、ファイアウォール6を介してインターネット1に接続されている。このデータベースサーバ5に対しては、認証された端末のみがファイアウォール6を介してアクセスすることができる。7は、インターネット1に接続された公開WWWサーバであり、認証、未認証を問わずいずれの端末であってもアクセス可能とされている。8は、

ファイアウォール6を介してインターネット1に接続された社内WWWサーバであり、この社内WWWサーバ8に対しては、認証された端末のみがファイアウォール6を介してアクセスすることができる。

【0007】図6は、従来のネットワークシステムにおける主要部の構成を示す図である。この図において、9は、クライアント側に設置されたクライアント端末であり、インターネット1に接続されている。このクライアント端末9は、インターネット1を介して後述するWWWサーバ13およびデータベースサーバ19へアクセスするものである。

【0008】クライアント端末9において、10は、クライアント端末9により実行されるクライアントアプリケーションプログラムであり、通信制御、暗号化制御、プロトコル制御等を行うためのプログラムである。また、クライアントアプリケーションプログラム10は、クライアント端末9からインターネット1を介して他の企業側のアプリケーションを利用するときに実行されるプログラムである。11は、暗号化通信制御部であり、予め定義された特定のプロトコルサービスポートを通過するデータグラムに対して、データ属性を問わず、暗号化、復号化を行うための暗号化専用プロトコルを制御する機能（例えば、SSL：Secure Socket Layer）を有している。12はセッションを管理するセッション管理部である。

【0009】WWWサーバ13は、ファイアウォール14を介してインターネット1に接続されており、クライアント端末9からの起動を契機として機能する端末である。ここで、ファイアウォール14には、複数のポートが設けられており、このポートとしては、未認証のクライアント端末9からのプロトコルを通す通常のポートと、認証済みのクライアント端末9からのプロトコルのみを通すセキュリティ通信用のポートに大別される。

【0010】上記WWWサーバ13において、15は、上述した暗号化通信制御部11と同様の機能を有する暗号化通信制御部である。16は、セッションを管理するセッション管理部である。17は、WWWサーバ13により実行されるサーバアプリケーションプログラムであり、クライアント端末9との間の通信制御等に用いられる。18は、後述するデータベース20に対するアクセス制御を行うDB（データベース）通信制御部である。データベースサーバ19は、記憶部にデータベース20を保持するものである。

【0011】ここで、図6に示すネットワークシステムの動作について、図7（a）および（b）に示す動作説明図を用いて説明する。図7（a）は、未認証の社外のクライアント端末91からのアクセス動作を説明する図であり、図7（b）は、未認証および認証済みのクライアント端末91および92からのアクセス動作を説明する図である。

【0012】ここで、図7(a)および(b)において、クライアント端末91は、図6に示す、未認証の他のクライアント端末9に対応しており、社外に設置されている。クライアント端末92は、図6に示す、認証済の他のクライアント端末9に対応しており、社外に設置されている。

【0013】図7(a)および(b)に示すファイアウォール14は、ポートPAおよびポートPBを有しており、このポートPAは、ポート番号として#80が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。従って、上記ポートPAのポート番号#80は、公知である。一方、ポートPBは、ポート番号としてポート番号#Xが付与されており、認証済みのクライアント端末92からのアクセスのために設定されているポートである。従って、ポートPBのポート番号#Xは、認証済のクライアント端末92のクライアントのみが通信に利用することができる番号である。言い換えれば、ポートPBには、特定のクライアント端末92からのみしかアクセスできない。

【0014】図7(a)および(b)に示す公開サーバ131および秘密サーバ132は、図6に示すWWWサーバ13に対応している。ここで、公開サーバ131には、インターネット1、ファイアウォール14のポートPAを介して、例えば、クライアント端末91がアクセスする。一方、秘密サーバ132には、インターネット1、14のポートPBを介して、例えば、クライアント端末92がアクセスする。21は、社内に設置されたクライアント端末であり、ファイアウォール14の内側におけるセキュリティが確保されているため、直接、公開サーバ131および秘密サーバ132へアクセス可能である。

【0015】図7(a)において、未認証のクライアント端末91は、通常、ファイアウォール14のポートPAを通過して公開サーバ131へhttp(Hyper Text Transfer Protocol)を用いてアクセスする。このとき、上記httpは、ポートPAを通過することができる。ここで、クライアント端末91から秘密サーバ132へのアクセスしようとした場合には、クライアント端末91のクライアントがポートPBのポート番号#Xを知らないため、ファイアウォール14を通過することができない。言い換えれば、クライアント端末91からのhttpは、ポートPBを通過することができないため、クライアント端末91と秘密サーバ132との間で通信が成立しないのである。従って、この場合には、クライアント端末91が秘密サーバ132へアクセスすることができないため、セキュリティが確保される。

【0016】一方、図7(b)において、クライアント端末92から秘密サーバ132へアクセスしようとした場合には、クライアント端末92は、セキュリティ通信専

用のプロトコルを用いて、まず、ポートPBへアクセスする。このとき、上記プロトコルがポートPBを通過することができるので、クライアント端末92は、秘密サーバ132へアクセスできる。

【0017】

【発明が解決しようとする課題】ところで、上述した従来のネットワークシステムにおいては、ファイアウォールを用いた、よりセキュアな企業間通信を実現することが、強いニーズとなっている。しかしながら、上述したネットワークシステムのファイアウォール環境においては、階層的に分散された組織分散型のファイアウォールが多段階構成で存在するため、1つの新しいプロトコルをファイアウォールを通過させるために、多大なる準備、運用稼働が必要となるという問題があった。この準備、運用稼働としては、図6に示すファイアウォールのポートの再設定、クライアントアプリケーションプログラム10、サーバアプリケーションプログラム17の仕様変更等が挙げられる。

【0018】ここで、図8を参照して、従来のネットワークシステムの問題点について詳述する。図8において、図7(a)および(b)に対応する部分には、同一の符号を付ける。図8に示す企業Aにおいて、14Aは、図7に示すファイアウォール14と同様の機能を有するファイアウォールであり、インターネット1(図6参照)と公開サーバ131Aおよび秘密サーバ132Aとの間に設けられている。ここで、ファイアウォール14Aは、ポートPAおよびポートPCを有している。

【0019】上記ポートPAは、ポート番号として#80が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。一方、ポートPCは、ポート番号としてポート番号#Yが付与されており、認証済みのクライアント端末92からのアクセス(分散コンピューティング通信)のために設定されているポートである。このポートPCは、セキュリティ専用ポートである。従って、ポートPCのポート番号#Yは、認証済のクライアント端末92のクライアントのみが通信に利用することができる番号である。言い換えれば、ポートPCには、特定のクライアント端末92からのみしかアクセスできない。21Aは、企業A内に設置されたクライアント端末であり、公開サーバ131Aおよび秘密サーバ132Aへアクセスする。

【0020】また、企業Bにおいて、14Bは、インターネット1と秘密サーバ132Bとの間に設けられたファイアウォールであり、共に分散コンピューティング通信専用のポートPCおよびポートPDを有している。上記ポートPCには、ポート番号#としてYが、ポートPDには、ポート番号#としてZが各々付与されている。ポートPCのポート番号#Yは、認証済のクライアント端末92のクライアントのみが通信に利用することができる番号である。これらのポートPCおよびPDは、セキュリ

ディ専用ポートである。

【0021】上記構成において、未認証のクライアント端末91は、通常、ファイアウォール14AのポートPAを通過して公開サーバ131Aへhttp（Hyper Text Transfer Protocol）を用いてアクセスする。このとき、上記httpは、ポートPAを通過することができる。なお、クライアント端末91は、上述した動作と同様に、ファイアウォール14AのポートPC、およびファイアウォール14BのポートPC、PDを通過して当該サーバへアクセスできない。

【0022】一方、クライアント端末92から秘密サーバ132Aへアクセスしようとした場合には、クライアント端末92は、セキュリティ通信専用のプロトコルを用いて、まず、ファイアウォール14AのポートPCへアクセスする。このとき、上記プロトコルがポートPCを通過することができるので、クライアント端末92は、秘密サーバ132Aへアクセスできる。

【0023】ここで、ファイアウォール14Bが既に他のサービスプロトコルのために割り当て済みである状態で、クライアント端末92がファイアウォール14BのポートPCを介して秘密サーバ132Bへアクセスした場合について説明する。この場合には、ポートPCがふさがっているため、ファイアウォール14Bにおいては、ポートPDを設定する必要がある。このポート設定の変更の情報は、クライアント端末92の管理者に通知される必要がある。ここで、クライアント端末92には、複数のファイアウォールにおけるポート設定情報を管理するポート管理部22が設けられている。

【0024】ここで、従来のネットワークシステム（図8参照）においては、分散コンピューティングを実現するために、必要とする全ての機能（サーバアプリケーション）が存在する全ての相手先システム（他企業内システム）に対してクライアント端末92等からのアクセスを可能とすべく、すべてのセキュリティポリシーを満足するためのセキュリティ制御が行われている。しかしながら、図8を参照して説明したように、従来のネットワークシステムにおいては、ポート設定変更のルールが企業によってまちまちであり、ポート管理部22への定義情報の管理が煩雑化するとともに、その制御が複雑になってしまう。従って、このようなポート設定の条件を加味して、業務単位に対応付けてアプリケーションの実行を行うためには、非常に複雑な実装方式を検討・開発せざるを得ない。特に、セキュリティ案件に関わる実装変更については、企業単位に重要かつ慎重な検討課題であり、これが早急なシステム実現への妨げになっている。本発明はこのような背景の下になされたもので、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0025】

【課題を解決するための手段】請求項1に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うことを特徴とする。また、請求項2に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第1のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第1のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第2のポートとして設定し、前記プロキシサーバは、前記クライアント端末から見たポートを前記第1のポートから前記第2のポートに変換する一方、前記サーバから見たポートを前記第2のポートから前記第1のポートに変換し、前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うことを特徴とする。また、請求項3に記載の発明は、請求項1または2に記載のネットワークシステムにおいて、前記クライアント端末に設けられ、前記データ通信におけるデータの暗号化および復号化を行う第1の暗号化通信制御部と、前記サーバに設けられ、前記データ通信におけるデータの暗号化および復号化を行う第2の暗号化通信制御部とを具備することを特徴とする。また、請求項4に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。また、請求項5に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第1のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第1のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第2のポートとして設定し、前記プロキシサーバは、前記クライアント端末から見たポートを前記第1のポートから前記第2のポートに変換する一方、前記サーバから見たポートを前記第2のポートから前記第1のポートに変換し、前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0026】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。図1は本発明の一実施形態によるネットワークシステムにおける主要部の構成を示す図である。この図において、図6の各部に対応する部分には同一の符号を付ける。図1に示す30は、クライアント側に設置されたクライアント端末であり、インターネット1に接続されている。このクライアント端末30は、インターネット1を介して後述するWWWサーバ34およびデータベースサーバ19へアクセスするものである。

【0027】クライアント端末30において、31は、

クライアント端末30により実行されるクライアントアプリケーションプログラムであり、通信制御、暗号化制御、プロトコル制御等を行うためのプログラムである。また、クライアントアプリケーションプログラム10は、後述する専用のプロトコルを用いるときに実行されるとともに、クライアント端末30からインターネット1およびファイアウォール35を介して他の企業側のアプリケーションを利用するときに実行されるプログラムである。

10 【0028】32は、分散コンピューティング通信制御部であり、後述するサーバアプリケーションプログラム38の一部を動的にクライアントアプリケーションプログラム31と関連づけたり、複製したりする。また、分散コンピューティング通信制御部32は、上記サーバアプリケーションプログラム38の一部をあたかもクライアント端末30に既存の業務アプリケーションプログラムのように扱えるような実行環境を実現するための、通信プロトコル機能を有している。33は、暗号化通信制御部であり、図6に示す暗号化通信制御部11と同一の機能を有している。

30 【0029】WWWサーバ34は、ファイアウォール35を介してインターネット1に接続されており、クライアント端末30からの起動を契機として機能する端末である。このファイアウォール35には、複数のポートが設定されているが、クライアント端末30が未認証であるか認証済であるかを問わず、クライアント端末30とWWWサーバ34との間の通信においては、ポート番号#80のポートが用いられる。このポート番号#80のポートは、公知であり、http等の一般的なプロトコルを通過させるためのものである。このファイアウォール35のポート設定状況および、クライアント端末30とWWWサーバ34との間の通信プロトコルの詳細については後述する。

40 【0030】上記WWWサーバ34において、36は、上述した暗号化通信制御部11と同様の機能を有する暗号化通信制御部である。37は、上述した分散コンピューティング通信制御部32と同様の機能を有する分散コンピューティング通信制御部である。38は、WWWサーバ34により実行されるサーバアプリケーションプログラムであり、クライアント端末30との間の通信制御等に用いられる。また、サーバアプリケーションプログラム38は、後述する専用のプロトコルを用いる場合に実行されるプログラムである。39は、データベース20に対するアクセス制御を行うDB（データベース）通信制御部である。

50 【0031】ここで、図1に示すネットワークシステムを企業間における分散コンピューティング通信に適用した場合の構成について図2を参照して説明する。図2に示すネットワークシステムは、企業A内のシステムと企業B内のシステムとがインターネット1（図1参照）を

介して接続されており、かつ該インターネット1には、未認証のクライアント端末301および認証済のクライアント端末302が接続されている。

【0032】ここで、図2に示すクライアント端末301は、図1に示す、未認証の一のクライアント端末30に対応しており、社外に設置されている。クライアント端末302は、図1に示す、認証済の他のクライアント端末30に対応しており、社外に設置されている。ここで、クライアント端末301および302の各記憶部には図1に示すクライアントアプリケーションプログラム31が記憶されている。

【0033】企業Aにおいて、ファイアウォール35Aは、図1に示すファイアウォール35に対応しており、ポートPAを有している。このポートPAは、ポート番号として#80が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。なお、実際には、ファイアウォール35Aは、論理的なポートが複数設けられており、それぞれのポートのポート番号は、任意に設定される。ただし、以下の説明において、用いられるポートは、ポート番号#80のもののみである。

【0034】341Aは、図1に示すWWWサーバ34に対応する公開サーバであり、インターネット1およびファイアウォール35Aを介してクライアント端末301によりアクセスされる。342Aは、図1に示すWWWサーバ34に対応する秘密サーバであり、後述する専用のプロトコルにより、インターネット1およびファイアウォール35A（ポートPA）を介して認証済のクライアント端末302によりアクセスされる。ここで、公開サーバ341Aおよび秘密サーバ342Bの各記憶部には、図1に示すサーバアプリケーションプログラム38が記憶されている。クライアント端末21Aは、企業A内に設けられており、公開サーバ341Aおよび秘密サーバ342Aに対してアクセスする。

【0035】一方、企業Bにおいて、ファイアウォール35Bは、図1に示すファイアウォール35に対応しており、ポートPAを有している。このポートPAは、ポート番号として#80が付与されている。このファイアウォール35Bの機能は、上述したファイアウォール35Aの機能と同一である。342Bは、専用のプロトコルにより、インターネット1およびファイアウォール35B（ポートPA）を介して、クライアント端末302によりアクセスされる。この秘密サーバ342Bの記憶部には、図1に示すサーバアプリケーションプログラム38が設けられている。クライアント端末21Bは、企業B内に設けられており、秘密サーバ342Bにアクセスする。

【0036】次に、上述した一実施形態によるネットワークシステムの動作について図3を参照して説明する。この図において、図2の各部に対応する部分には同一の符号を付けその説明を省略する。この図においては、図

2に示す認証済のクライアント端末302がインターネット1および企業A内のファイアウォール35Aを介して秘密サーバ342Aにアクセスする例について図示されている。また、図3に示すファイアウォール35Aにおいては、ポートPAと、該ポートPAとは異なるポートpAとが備えられているが、上記ポートPAとポートpAは、いずれもポート番号#80が時間的にずれて付与される。すなわち、ファイアウォール35Aにおいては、ポート番号#80が付与されるポートが変化する。

【0037】また、図3に示すクライアントアプリケーションプログラム（AP）42は、図1に示すクライアントアプリケーションプログラム31に相当するものであり、ドライバ（RApp_C）43を有している。このドライバ43は、クライアントアプリケーションプログラム42により実現される機能の一部であり、クライアント端末302と秘密サーバ342Aとの間のプロトコルシーケンスを制御するものである。

【0038】また、専用サーバプロセスプログラム（Regist）44は、サーバアプリケーションプログラム38の一部をなすプログラムであり、秘密サーバ342Aとクライアント端末302との間の通信制御を行うためのものである。この専用サーバプロセスプログラム44は、リモートオブジェクトプログラム（stub）45と通信制御プログラム（Skel）46とから構成されている。

【0039】このリモートオブジェクトプログラム45は、ファイアウォール35Aおよびインターネット1を介してクライアント端末302へ転送された後、クライアント端末302により実行されるプログラムであり、通信制御を行うためのものである。一方、通信制御プログラム46は、秘密サーバ342Aにより実行されるプログラムであり、リモートオブジェクトプログラム45と対をなして、通信制御を行うためのものである。

【0040】上記構成において、秘密サーバ342Aが起動されると、専用サーバプロセスプログラム44が実行され、秘密サーバ342Aは、動作可能状態とされる。この状態において、手順SA1では、クライアント端末302から、http40および認証済であることを示すクライアント認証データがファイアウォール35Aへインターネット1を介して送出される。今、ファイアウォール35AのポートPAにポート番号#80が付与されているものとする、上記http40は、ファイアウォール35AのポートPAを通過して、秘密サーバ342Aに入る。

【0041】これにより、秘密サーバ342Aは、クライアント端末302が認証済の端末であるか否かを、最初に送受される通信データの一部に含まれるクライアント認証データから判断し、サーバ側の認証に失敗したとき、以後の動作を行わない。今の場合、秘密サーバ342Aは、クライアント端末302が認証済の端末であるた

め、httpd (http daemon) 41により、クライアントアプリケーションプログラム42を認識する。

【0042】そして、手順SA2では、秘密サーバ342Aは、上記クライアントアプリケーションプログラム42をポートPAおよびインターネット1を介してクライアント端末302へJava Applet等の形態をとってダウンロードする。これにより、クライアント端末302においては、クライアントアプリケーションプログラム42が実行されることにより分散コンピューティング通信が開始される。

【0043】次に、手順SA3では、クライアント端末302は、ドライバ43を用いて、分散コンピューティング通信で用いるファイアウォール35Aにおけるポート(番号)の情報をインターネット1およびポートPAを介して秘密サーバ342Aへ要求する。これにより、手順SA4では、秘密サーバ342Aは、ポートとしてポートPAに代えてポートpAを予約するとともに、該ポートpAにポート番号#80を付与する。すなわち、この予約により、ポート番号#80のポートは、ポートPAからポートpAに変更されたのである。以後のプロトコルシーケンスは、すべてポートpA(ポート番号#80)を介して行われる。

【0044】次に、手順SA4では、秘密サーバ342Aは、プロトコルシーケンスを行うポートとして予約されたポートpA(ポート番号#80)の情報をポートpAおよびインターネット1を介してクライアント端末302へ送出する。これにより、クライアント端末302は、以後に使用するファイアウォール35AのポートがポートpA(ポート番号#80)であることを認識する。

【0045】次に、手順SA5では、秘密サーバ342Aは、指定されたポートpA(ポート番号#80)を介しての通信に必要なリモートオブジェクトプログラム45のダウンロードを要求するための情報をインターネット1およびポートpAを介して秘密サーバ342Aへ送出する。これにより、手順SA6では、秘密サーバ342Aは、リモートオブジェクトプログラム45をポートpAおよびインターネット1を介してクライアント端末302へダウンロードする。

【0046】これにより、クライアント端末302において、リモートオブジェクトプログラム45が実行される。以後、手順SA7～手順SA10のように、クライアント端末302と秘密サーバ342Aの間では、インターネット1およびファイアウォール35AのポートpAを介してデータ通信が行われる。また、このデータ通信においては、図1に示す暗号化通信制御部33、36によりデータの暗号化、復号化が行われているので、セキュアな通信が実現できる。

【0047】以上説明したように、上述した一実施形態によるネットワークシステムによれば、専用のプロトコルを用いることにより、ファイアウォール35Aにお

るポートを常にポート番号#80のポートとするように構成したので、クライアント端末302におけるポート管理が不要となる。このことから、上述した一実施形態によるネットワークシステムによれば、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムを得ることができるという効果が得られる。また、上述した一実施形態によるネットワークシステムによれば、既存のイントラネットセキュリティ・ポリシーに特別な設定変更を行うことなく、それまで通過を認めていなかった分散コンピューティング通信を安全に利用することができるという効果が得られる。

【0048】また、上述した一実施形態によるネットワークシステムによれば、ファイアウォール35Aのポートを通過させた全てのデータに対してプロトコルレベルで暗号化、復号化が施されることにより、運用的な利便性を実現することができるという効果が得られる。さらに、上述した一実施形態によるネットワークシステムによれば、企業に個々に確立されているイントラネット設計に大きな変更を加える必要がないため、関連企業間で設計検討・実装等を極めて短期間で完了させることができ、ひいてはこれらをつなぐ分散システムの構築を短期間で行うことができるという効果が得られる。

【0049】以上本発明の一実施形態によるネットワークシステムについて詳述してきたが、具体的な構成はこの一実施形態に限られるものではなく本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、上述した一実施形態によるネットワークシステムにおいては、図3に示す構成について説明したが、これに代えて図4に示す構成のものを採用してもよい。

【0050】以下、図4に示すネットワークシステムについて説明する。図4において、図3の各部に対応する部分には同一の符号を付けその説明を省略する。図4においては、プロキシサーバ47が新たに設けられている。また、図4においては、ファイアウォール35Aは、ポート番号#80のポートPAと、該ポートPAと異なるポート番号のポートPBとを有している。上記ポートPBのポート番号は、例えば、#Xとされている。

【0051】プロキシサーバ47は、ファイアウォール35A(または、秘密サーバ342A)に設けられており、企業A側のプライベートネットワークからインターネット1等のパブリックなネットワークに、またはその逆の場合に情報の通過を許可しないという役目をするサーバである。図4においては、プロキシサーバ47は、ポートPAに入力された情報をポートPBを介して秘密サーバ342Aへ出力する一方、ポートPBに入力された情報をポートPAを介してインターネット1へ出力するという、ポート変換機能を有している。すなわち、プロキシサーバ47により、クライアント端末302から秘密

サーバ342Aを見た場合、アクセス可能なポートがポートPAとされる一方、秘密サーバ342Aから秘密サーバ342Aを見た場合、アクセス可能なポートがポートPBとされる。

【0052】上記構成において、秘密サーバ342Aが起動されると、専用サーバプロセスプログラム44が実行され、秘密サーバ342Aは、動作可能状態とされる。この状態において、手順SB1では、クライアント端末302から、http40がファイアウォール35Aへインターネット1を介して送出される。今、ファイアウォール35AのポートPAにポート番号#80が付与されているものとする、上記http40は、ファイアウォール35AのポートPAを通過して、秘密サーバ342Aに入る。これにより、秘密サーバ342Aは、前述した動作と同様にして、httpd41により、クライアントアプリケーションプログラム42を認識する。

【0053】そして、手順SB2では、秘密サーバ342Aは、上記クライアントアプリケーションプログラム42をポートPAおよびインターネット1を介してクライアント端末302へJava Applet等の形態をとってダウンロードする。これにより、クライアント端末302においてはクライアントアプリケーションプログラム42が実行されることにより分散コンピューティング通信が開始される。

【0054】次に、手順SB3では、クライアント端末302は、ドライバ43を用いて、分散コンピューティング通信で用いるファイアウォール35Aにおけるポート(番号)の情報をインターネット1およびポートPAを介して秘密サーバ342Aへ要求する。これにより、手順SB4では、秘密サーバ342Aは、自身が使用するポートとして、ポートPB(ポート番号#X)を予約するとともに、該ポートPB(ポート番号#X)の情報をプロキシサーバ47に送出する。また、秘密サーバ342Aは、クライアント端末302が使用するポートとしてポートPA(ポート番号#80)の情報をポートPAおよびインターネット1を介してクライアント端末302へ送出する。

【0055】これにより、プロキシサーバ47においては、ポートPA→ポートPB(ポートPA→ポートPB)というポート変換が定義される。この定義により、秘密サーバ342Aからクライアント端末302を見た場合のプロトコルシーケンスが、ファイアウォール35AのポートPB上で行われる一方、クライアント端末302から秘密サーバ342Aを見た場合のプロトコルシーケンスは、ファイアウォール35AのポートPA上で行われる。つまり、秘密サーバ342Aは、分散コンピューティング通信を行うポートとしてポートPB(ポート番号#X)を認識している一方、クライアント端末302は、上記ポートとしてポートPA(ポート番号#80)を認識している。

【0056】次に、手順SB5では、秘密サーバ342Aは、指定されたポートPA(ポート番号#80)を介しての通信に必要なリモートオブジェクトプログラム45のダウンロードを要求するための情報をインターネット1へ送出する。これにより、プロキシサーバ47においてポート変換(ポートPA→ポートPB)が行われ、上記情報は、ポートPA、ポートPBを介して秘密サーバ342Aに入力される。

【0057】これにより、手順SB6では、秘密サーバ342Aは、リモートオブジェクトプログラム45をポートPBを介して送出する。このとき、プロキシサーバ47により、ポート変換(ポートPB→ポートPA)が行われ、上記リモートオブジェクトプログラム45は、ポートPB、ポートPAおよびインターネット1を介してクライアント端末302へダウンロードされる。

【0058】これにより、クライアント端末302において、リモートオブジェクトプログラム45が実行される。以後、手順SB7～手順SB10のように、クライアント端末302と秘密サーバ342Aの間では、インターネット1およびファイアウォール35AのポートPA、ポートPBを介してデータ通信が行われる。また、このデータ通信においては、図1に示す暗号化通信制御部33、36によりデータの暗号化、復号化が行われているので、セキュアな通信が実現できる。

【0059】また、上述した一実施形態によるネットワークシステムにおいては、上述した機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するように構成してもよい。なお、ここでいうコンピュータシステムとは、OS(オペレーティングシステム)や周辺機器等のハードウェアを含むものとする。また、コンピュータシステムは、WWWシステムを利用しているものであれば、ホームページ提供環境(または表示環境)を含むものとする。

【0060】

【発明の効果】以上説明したように、本発明によれば、専用プロトコルを用いることにより、ファイアウォールにおけるポートを常に公知のポート番号のポートとるように構成したので、クライアント端末側におけるポート管理が不要になる。このことから、本発明によれば、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムを得ることができるという効果が得られる。また、請求項3に記載の発明によれば、第1および第2の暗号化通信制御部によりデータの暗号化、復号化が行われているので、セキュアな通信を実現できるという効果が得られる。

【図面の簡単な説明】

【図1】 本発明の一実施形態によるネットワークシス

17

テムの主要部の構成を示す図である。

【図2】 同一実施形態によるネットワークシステムを企業間における分散コンピューティング通信に適用した場合の構成を示す図である。

【図3】 同一実施形態によるネットワークシステムの動作を説明する図である。

【図4】 同他の実施形態によるネットワークシステムの構成および動作を説明する図である。

【図5】 従来のネットワークシステムの概略構成を示す図である。

【図6】 従来のネットワークシステムの主要部の構成を示す図である。

【図7】 従来のネットワークシステムの動作を説明する図である。

【図8】 従来のネットワークシステムの問題点を説明する図である。

【符号の説明】

1 インターネット

30、301、302 クライアント端末

*

18

* 31 クライアントアプリケーションプログラム

32 分散コンピューティング通信制御部

33 暗号化通信制御部

34 WWWサーバ

341A 公開サーバ

342A、342B 秘密サーバ

35、35A、35B ファイアウォール

36 暗号化通信制御部

37 分散コンピューティング通信制御部

10 38 サーバアプリケーションプログラム

39 DB通信制御部

40 http

42 クライアントアプリケーションプログラム

43 ドライバ

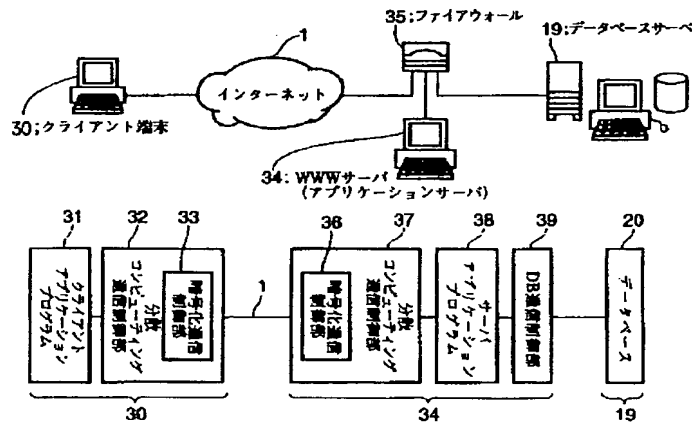
44 専用サーバプロセスプログラム

45 リモートオブジェクトプログラム

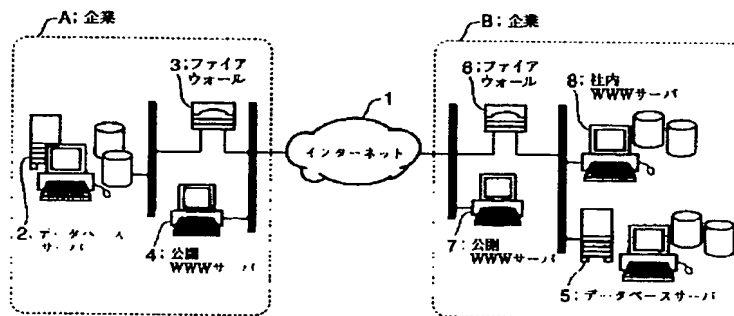
46 通信制御プログラム

47 プロキシサーバ

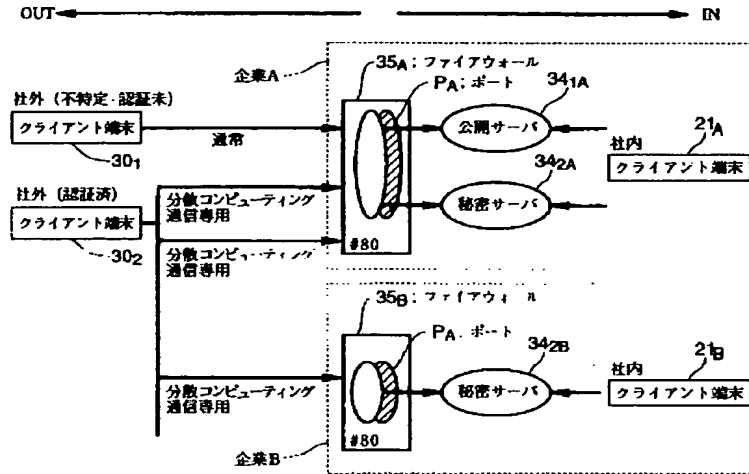
【図1】



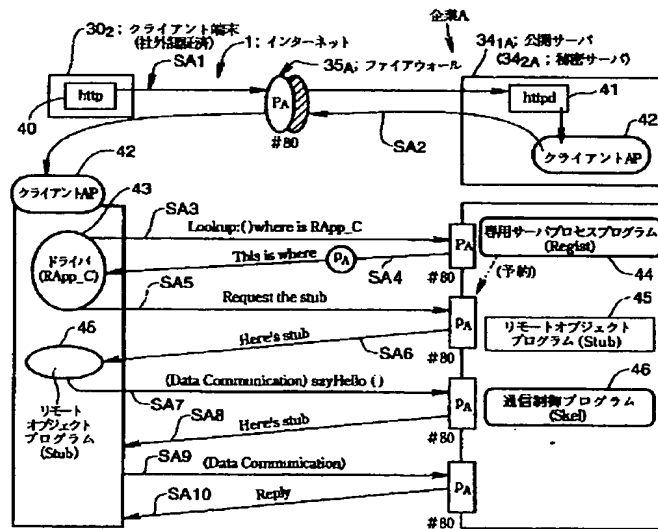
【図5】



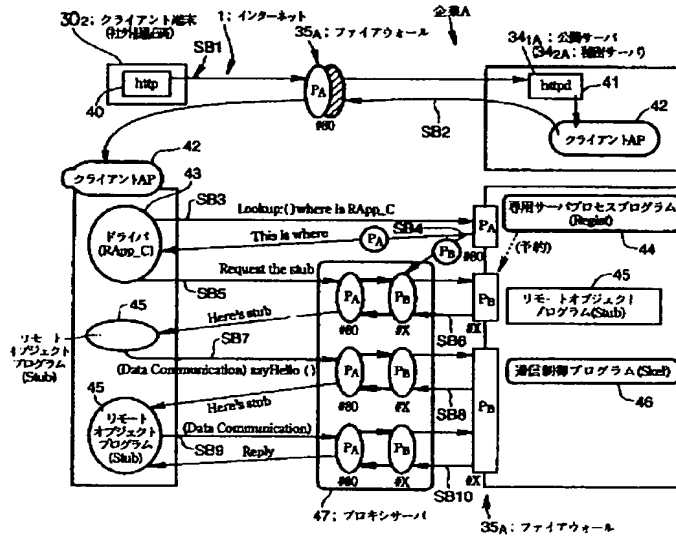
【図 2】



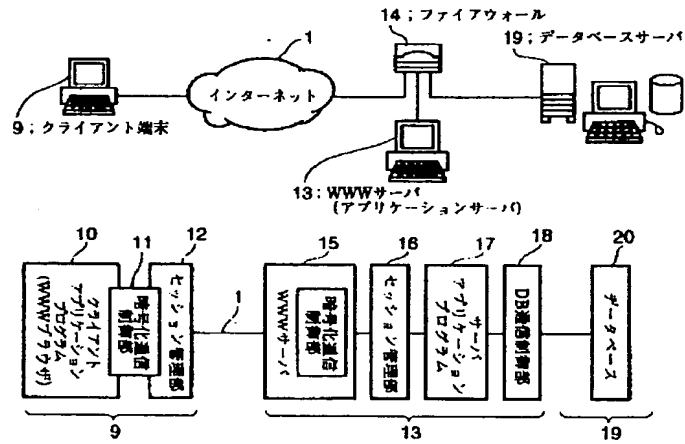
【図 3】



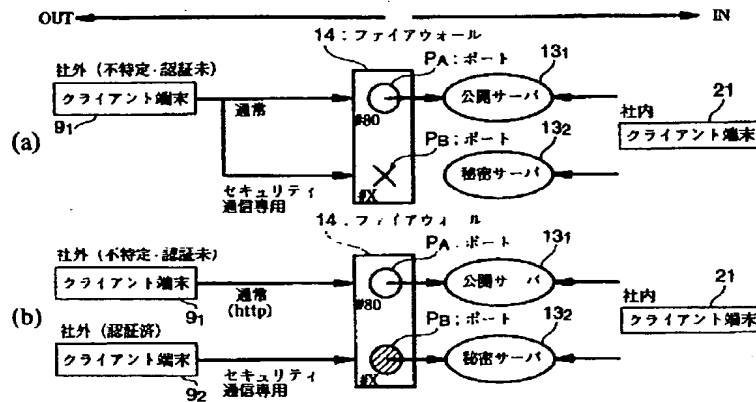
【図4】



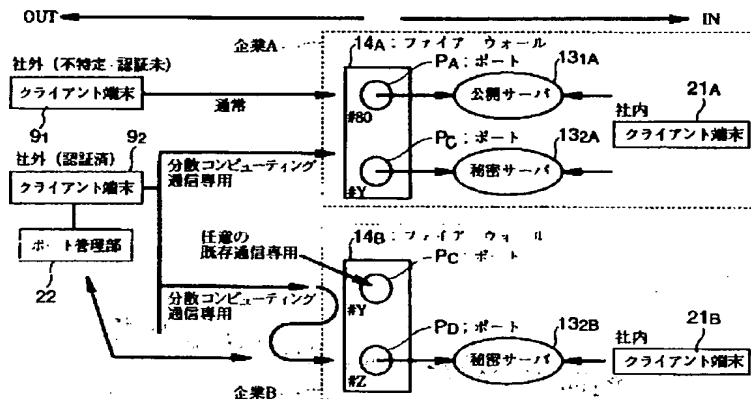
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 小林 和恵
 東京都港区港南一丁目9番1号 エヌ・テ
 ィ・ティ・コミュニケーションウェア株式
 会社内

This Page Blank (uspto)